Book of Knowledge

Author: Maurice Schippers • Course: ICS-CS4 • Class: RB02-Eindhoven

A book with numbers coming out of it

Description automatically generated

|  |  |  |
| --- | --- | --- |
| Version | Date | Changes |
| 1 | 17-09-2023 | + Added 1. Introduction  + Added 1.2 Basic Hacking and Pentesting Process  \* Working on 1.3 Threat + Risk Analysis and CIA |
| 1.1 (current) | ??? | + Added 1.2.1 Threat Analysis |

Table of Contents:

[1 Introduction and Personal BoK Approach 3](#_Toc145976871)

[1.1 Basic Hacking and Pentesting Process 3](#_Toc145976872)

[1.1.1 Pentest Goals and Contract (Preparation) 3](#_Toc145976873)

[1.1.2 Pentest Process (Execution) 4](#_Toc145976874)

[1.1.3 Pentest Report (Reporting) 5](#_Toc145976875)

[1.2 Threat + Risk Analysis and CIA 5](#_Toc145976876)

[1.2.1 Threat Analysis 5](#_Toc145976877)

[2 Web: Application Attack and Defense 7](#_Toc145976878)

[2.1 Footprinting, Reconnaissance and Social Engineering 7](#_Toc145976879)

[2.2 Path Traversal, (remote) File inclusion and Command Injection 7](#_Toc145976880)

[3 Web: Database Attack and Defense 8](#_Toc145976881)

[3.1 Web Application Firewalls 8](#_Toc145976882)

[3.2 SQL Injection 8](#_Toc145976883)

[4 Web: Site Attack and Defense 9](#_Toc145976884)

[4.1 Host Intrusion Detection and Prevention (HIDS) 9](#_Toc145976885)

[4.2 XSS & CSRF 9](#_Toc145976886)

[5 Network: Identification of Vulnerabilities 10](#_Toc145976887)

[5.1 Network Scanning and Enumeration (incl. Sniffing) 10](#_Toc145976888)

[5.1.1 How to securely host a Web Shop with Secure Network Connections (HTTPS/TLS/SSH) 10](#_Toc145976889)

[5.2 Law & Ethics and Responsible Disclosure + GDPR 10](#_Toc145976890)

[6 Network: Protect the Network 11](#_Toc145976891)

[6.1 Network Separation and Segmentation 11](#_Toc145976892)

[6.2 VPN: How to manage a Web Shop with Secure Remote Access 11](#_Toc145976893)

[7 Network: Attack the Network 12](#_Toc145976894)

[7.1 Network Spoofing and Man in The Middle Attacks (MITM) 12](#_Toc145976895)

[7.2 WiFi Hacking 12](#_Toc145976896)

[8 Network: Monitor and Detect 13](#_Toc145976897)

[8.1 Network Intrusion Detection and Prevention (NIDS/IPS) 13](#_Toc145976898)

[8.2 IT Monitoring 13](#_Toc145976899)

[8.2.1 IT Basic Monitoring (Availability) 13](#_Toc145976900)

[8.2.2 IT Security Monitoring (Confidentiality and Integrity) 13](#_Toc145976901)

[9 Concepts: Identity Management, Authentication and Access Control 14](#_Toc145976902)

[9.1 Identity Management, Authentication and Access Control 14](#_Toc145976903)

[9.2 Password Cracking (system and network) 14](#_Toc145976904)

[10 Concepts: Incident Response and Analysis 15](#_Toc145976905)

[10.1 Security Incident Management 15](#_Toc145976906)

[10.2 IT System Hardening + Common Vulnerabilities and Exposures (CVE's) 15](#_Toc145976907)

[11 Overall Conclusion 16](#_Toc145976908)

[12 References 17](#_Toc145976909)

# Introduction and Personal BoK Approach

Welcome to my personal Book of Knowledge (BoK) document. My name is Maurice Schippers, and I am a student in the Cyber Security specialization course. I have always had a passion for this subject ever since I started my career in ICT. I enjoy solving puzzles and I think security is one of the most important aspects of IT considering how many people use computers of any type nowadays and the vulnerability of the data that is stored everywhere. Also, with the rise of AI on the horizon, it will become more challenging to defend, and it has proven to be much easier for black-hat hackers to create malware tools (Sabin, 2023). This motivates me to keep on learning and improving my skills.

This document serves as a reflection of my learning progress through the different subjects. For each of the subjects, I will be gathering information from different sources, starting with Canvas, and branch out from there when needed. I also aim to get some hands-on experience for each of the subjects. After all: “*Theory will take you only so far*”.

## Basic Hacking and Pentesting Process

A general pentest process can be defined in three stages: Preparation (Defining goals and scope and setting up a contract), Execution (Conducting the tests) and Reporting (Delivering and presenting a report based on the test results).

### Pentest Goals and Contract (Preparation)

Each penetration test process generally starts with finding out what the client really wants/needs.

1. Setting goals: Finding out what the client wants to achieve and what their objectives for the tests are. It is also possible to define success criteria, to further narrow down the goals of the client.
2. Setting scope: Setting boundaries, maintaining a focused approach, and determining the specific areas and methods to be used.
3. Types of testing: Ethical hackers must consider various types of testing methodologies when defining the scope of a penetration test. The choice of testing type heavily influences the approach and tactics used during the assessment. Common types of testing include:
   1. Black-Box Testing: This approach involves testing without any prior knowledge of the target systems or applications. Ethical hackers simulate an attacker with no inside information, relying completely on external sources.
   2. Gray-Box Testing: In this approach, ethical hackers have limited information about the target, such as IP addresses and server locations. This approach is a balance between black-box and white-box testing.
   3. White-Box Testing: Ethical hackers have full access to internal details, including source code and configuration settings. This type of testing offers a full view of the system's security.
   4. Crystal Box Testing: Similar to white-box testing, but it may involve access to more sensitive information. This level of access allows for an in-depth analysis of security components.
   5. Social Engineering Tests: In certain cases, clients may request social engineering tests to assess the effectiveness of security awareness and incident response within their company. For these tests phishing or vishing simulations could be used. However, it is important to remember that this is part of the *Exploitation* phase and could potentially be harmful.
4. Client reassurance: Making clear to the client that the penetration test will be conducted with utmost care and that no intrusive tests will be performed on operational environments unless explicitly requested by the client. In cases where intrusive tests or real exploitation are part of the assessment, they will be conducted in isolated test or acceptance environments designed to reflect the operational environment accurately. This is done during the first contact but possibly remains relevant later in the process as well.

After that, a contract can be established with the client. This contract requires, at minimum, the following aspects:

1. Indemnification Clause: This clause is typically signed by the client and allows ethical hackers to conduct the tests. It also addresses liability. This clause is very important because while testers assume responsibility for careful testing, any remaining risk associated with testing lies with the client. Testers cannot be held liable for damages resulting from the testing.
2. Confidentiality Agreement: All testers should sign a confidentiality agreement to ensure the protection of sensitive information and data gathered during the assessment.
3. Scope and Tested Systems: Provide detailed information about the scope of the assessment, including tested systems and environments. This information should include location, IP ranges, DNS names, and other relevant details.
4. Test Origin and Testing Times: Specify the origin of the tests, including the IP address from which tests will be performed. Additionally, define the testing times or periods to allow the client to check and distinguish these tests from potential real attacks.
5. Incident/Emergency Escalation Procedure: Make a clear plan for an escalation procedure to follow in the case of incidents or emergencies, allowing for a smooth and efficient response to unexpected situations.

### Pentest Process (Execution)

The execution of a pentest usually follows five stages:

1. Intel Gathering (Reconnaissance Part 1): Collecting information about the target, which may include company details such as phone numbers, names, email addresses, websites, and more.
2. Footprinting (Reconnaissance Part 2): This phase is also part of Reconnaissance but goes deeper and involves identifying and understanding the digital *footprint* of the target. It includes aspects such as the network (IP ranges, active IP addresses, open ports, OS versions), as well as critical servers and system architecture.
3. Vulnerability Analysis: Ethical hackers analyse and assess vulnerabilities within the target systems, prioritizing them based on severity and potential impact.
4. Exploitation: Although typically excluded from standard pentests, if requested by the client, ethical hackers will attempt to access the system through identified vulnerabilities, gaining unauthorized control or access. These tests can potentially disrupt services and are therefore usually only performed in controlled testing environments to protect the integrity of the system.
5. Post-Exploitation and Clean-Up: This step is rarely included in pentests, especially since the majority of pentests do not involve exploitation. In scenarios where it would be applicable, this stage would consist of actions like data manipulation, log clearing, or evidence removal—a pattern often followed by malicious hackers to hide their activities.

### Pentest Report (Reporting)

The final phase is the reporting phase, where the observations are documented and discussed with the client through a detailed report and presentation:

1. Reporting: The report should cover certain specific elements, including:
   1. Scope and Goals: It contains the specific scope and objectives of the pentest to provide context.
   2. Test Approach: A clear explanation of the chosen testing approach is provided, detailing the methodologies and techniques used during the test.
   3. Test Results: Test results, including identified vulnerabilities and security issues. Each finding is explained in detail to help the client understand why it is an issue.
   4. Overall Conclusions: The report concludes with an overall assessment, like giving recommendations and guidance on how to address the identified security issues. Basically, proposing solutions to the client.
2. Presenting: A presentation is usually done for the client, and potentially other stakeholders, including management and technical experts. During this presentation, ethical hackers explain the findings and conclusions of the pentest in-depth, providing an opportunity for direct interaction and discussion. It is important to keep in mind that not everyone involved has a technical background.

## Threat + Risk Analysis and CIA

TODO

### Threat Analysis



I have decided to analyze the international company eBay because it is such a large and well-known company. eBay is an American e-commerce company where users can buy and sell items, both new and used, through consumer-to-consumer (C2C) and business-to-consumer (B2C) transactions. As of 2023, eBay is estimated to have 129 million active users (*EBay Revenue and Usage Statistics (2023) - Business of Apps*, 2023). Each of these factors plays a role in the potential risks associated with the company.

|  |  |  |  |
| --- | --- | --- | --- |
| **Dimension** | **Information Attribute** | **Threat** | **Relevance for eBay** |
| **C**onfidentiality | Exclusiveness | Disclosure | Considering eBay holds the data of millions of users, an unauthorized disclosure could not only put customers at risk of financial fraud or identity theft but also inflict substantial reputational damage on the company, damaging user trust. |
|  | Exclusiveness | Abuse | Abuse of customer data can result in direct harm to the individuals, whereas misuse of employee data or internal company information could escalate into more significant business and security issues. |
| **I**ntegrity | Correct | Tampering | Prices and user data should be kept intact because of the significance of the transactions. |
|  | Complete | Removal | Removal of data, like products or user data, could result in confusing and more importantly, of money. |
|  | Complete | Addition | This could result in a fake product or account, that could be used to lure in the money of an unexpecting customer. |
|  | Valid | Out of date | Outdated information, like displaying products that have already been sold or referencing deleted accounts, can lead to confusion and frustration among users. This is especially important for user trust and user “goodwill”. |
|  | Authentic | Forgery | Like the addition of fake information, unsuspecting customers could be baited to pay money or lead to external sites, while thinking they are still on eBay. |
|  | Indisputability | Denial | If users can't access their own data or see products they want to buy, they might get frustrated. This could make them trust eBay less, and switch to another platform, making the company lose money. |
|  | Consistency | Inconsistency | (Sudden) differences in product info, prices, or purchase history can confuse users and might cause money-related issues. |
| **A**vailability | Well timed | Delay | If there's a delay in updating product listings or processing transactions, customers could miss out on purchases. This kind of delay could frustrate users and lead to a decrease in sales. |
|  | Continuity | Downtime | Downtime can lead to a significant loss in sales, because of the huge number of transactions that happen every day. Long or frequent downtimes can also damage trust and make customers consider other competing platforms. |

* Perform a qualitative risk analysis for the company environment that you are analysing and developing this semester.  
  Note: You can use the excel sheet or word document for the risk analysis (see sources) if you want to.  
  1. List and describe the threats for your company in terms of possible attackers (threat actors) and their motivations.  
  2. For each threat determine and explain the probability (likelihood) on a qualitative scale, e.g.:  
       Unlikely: Not expected in the coming year;  
       Likely: Could happen the coming year,  
       Very Likely: Will probably happen the coming year.  
  3. For each threat determine and describe the possible impacts if it occurs. Determine the impact in terms of down-time, damage to customers, physical damage, reputation damage, possible claims or fines, incident handling costs (hours), environmental damage, human safety (injuries or loss of human lives). Explain why and how this impact can happen for your company.
* Add the risk analysis, with the chosen set of controls to your Body of Knowledge:  
  - Explain your analysis and choices for controls.  
  - Show (in for example a cross-reference table) how the controls are related to the threats or risks.  
  - Also show which of the controls you have actually implemented in your demo network.  
  - Add an introduction and conclusions to your Body of Knowledge document.
* Make a list of both quantitative and qualitative methods that you can find online. Analyse and Discuss differences / strengths of each method and the typical applications of the method (who uses it, what for?). Select the method that best fits your environment and perform a risk analysis with that method.

# Web: Application Attack and Defense

## Footprinting, Reconnaissance and Social Engineering

x

## Path Traversal, (remote) File inclusion and Command Injection

x

# Web: Database Attack and Defense

## Web Application Firewalls

x

## SQL Injection

x

# Web: Site Attack and Defense

## Host Intrusion Detection and Prevention (HIDS)

x

## XSS & CSRF

x

# Network: Identification of Vulnerabilities

## Network Scanning and Enumeration (incl. Sniffing)

x

### How to securely host a Web Shop with Secure Network Connections (HTTPS/TLS/SSH)

x

## Law & Ethics and Responsible Disclosure + GDPR

x

# Network: Protect the Network

## Network Separation and Segmentation

x

## VPN: How to manage a Web Shop with Secure Remote Access

x

# Network: Attack the Network

## Network Spoofing and Man in The Middle Attacks (MITM)

x

## WiFi Hacking

x

# Network: Monitor and Detect

## Network Intrusion Detection and Prevention (NIDS/IPS)

x

## IT Monitoring

Split on CIA:

### IT Basic Monitoring (Availability)

x

### IT Security Monitoring (Confidentiality and Integrity)

x

# Concepts: Identity Management, Authentication and Access Control

## Identity Management, Authentication and Access Control

x

## Password Cracking (system and network)

x

# Concepts: Incident Response and Analysis

## Security Incident Management

x

## IT System Hardening + Common Vulnerabilities and Exposures (CVE's)

x

# Overall Conclusion

# References

*EBay Revenue and Usage Statistics (2023) - Business of Apps*. (2023, August 2). Business of Apps. https://www.businessofapps.com/data/ebay-statistics/

Sabin, S. (2023, January 10). *Hackers are already abusing ChatGPT to write malware*. Axios. Retrieved September 11, 2023, from https://www.axios.com/2023/01/10/hackers-chatgpt-malware-cybercrime-ai